



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/059,182	01/31/2002	Janne Suuronen	004770.00521	5357
22907	7590	02/06/2008	EXAMINER	
BANNER & WITCOFF, LTD. 1100 13th STREET, N.W. SUITE 1200 WASHINGTON, DC 20005-4051			SHAW, YIN CHEN	
		ART UNIT	PAPER NUMBER	
		2139		
		MAIL DATE	DELIVERY MODE	
		02/06/2008	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/059,182	SUURONEN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 31 October 2007.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1,4-6,11,32-34,40-50,53,54 and 56-63 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1, 4-6, 11, 32-34, 40-50, 53-54, and 56-63 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    - a) All    b) Some \* c) None of:
      1. Certified copies of the priority documents have been received.
      2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
      3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____.                                     |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____.   | 6) <input type="checkbox"/> Other: _____.                         |

## DETAILED ACTION

1. This written action is responding to the Request for Continued Examination (RCE) dated on 10/31/2007.
2. Claims 1, 4-6, 11, 32-34, 40-50, 53-54, and 56-63 have been submitted for examination.
3. Claims 1, 4-6, 11, 32-34, 40-50, 53-54, and 56-63 are currently pending.

In response to Applicant's remark that Fink et al. fails to disclose the argued limitation, "classify the received data packets based on the contents of the data packet", Examiner respectfully disagrees with it. Fink et al. specifically teaches "**inspects the contents of such packet or packets (see line 67, Col. 6)**". The newly amended claims are now rejected with the prior cited reference in combination with the newly found reference by Makinson et al. (U.S. Patent 7,023,861). Please refer to rejections below.

## Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 4, 32-34, 40-50, 53, 56, 58, and 60-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Makinson et al. (U.S. Patent 7,023,861).

i. Referring to Claims 1, 49, 50, 62:

As per Claim 1, Fink et al. disclose an apparatus comprising:  
a firewall [(fig. 1)] configured to:  
receive data packets over a first network [Packets which are permitted to pass through gateway 15 from external network 14 are then received by one of a plurality of protected nodes 20 (lines 335-37, Col. 5)];  
classify the received data packets based on the contents of the data packets into packets of a first type and second type [inspects the contents of such packet or packets (line 67, Col. 6). Pre-filtering module 30 also preferably features a classification engine 38, including a data processor, for at least partially analyzing the information from the packet (lines 4-6, Col. 8)];  
Fink et al. do not expressly disclose the remaining limitations of the claim. However, Makinson et al. disclose packets which cannot contain virus and packets which can contain a virus and the virus scanning engine for testing if the packet contains virus [The malware scanner 16 is illustrated in the form of a software based scanner using a general purpose computer

formed of a central processing unit 58 (lines 57-59, Col. 5). In contrast to the highly programmable and flexible software scanner 16, a hardware based scanner 16' may also be provided. The software based scanner 16 could perform non-time critical scanning such as SMTP scanning whereas an optional high performance hardware scanner 16' could be provided, for example, to scan for computer viruses with NFS application layer protocol data packets (lines 18-24, Col. 6)] and forward the data packets of the first type to a destination without testing by a virus scanning engine and forward the data packets of the second type of a virus scanning engine for testing [The data packet analyzer can be responsive to different properties of the data packets to determine whether or not they are to be passed to the malware scanner (lines 50-52, Col. 2). At step 20 the network bridge 14 checks to see if the data packet is one that is to pass through the network bridge 14 or is alternatively intended for a recipient on the same side of the network bridge 14 as the packet was received. If the data packet is not to pass through the network bridge 14, then processing is returned to step 18 to await receipt of the next data packet. If the data packet is to pass through the network bridge 14, then step 22 serves to identify the network layer protocol associated with that data packet. At

step 24 this network layer protocol is checked to see if it is one which is to be scanned by the associated malware scanner 16 (lines 34-45, Col. 4)]. Fink et al. and Makinson et al. are analogous art because they are from similar technology relating to information security and packet scanning. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine the system disclosed in Fink et al. with Makinson et al. since one would have been motivated to realize that as computer systems and computer networks become increasingly important to their users, the threat posed by malware, such as computer viruses, Trojans, worms, banned computer programs or abusive e-mails, becomes increasingly significant and Malware scanners are an important form of defence against such problems (lines 23-28, Col. 1 from Makinson et al.). Therefore, it would have been obvious to combine Fink et al. with Makinson et al. to obtain the invention as specified in Claim 1.

As per Claim 49, it is a method claim that corresponds to the apparatus claim 1. Therefore, Claim 49 is rejected for the same rationale as of Claim 1.

As per Claim 50, it is storage medium claim that corresponds to the apparatus claim 1. In addition, Fink et al. disclose a computer

program stored on a storage medium [The device comprising: (a) a memory for storing at least one instruction (lines 22-23, Col. 3). The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3)]. Therefore, Claim 50 is rejected for the same rationale as of Claim 1.

As per Claim 62, it is an apparatus claim that shares similar limitations as of claim 1. In addition, Fink et al. disclose memory and processor [The device comprising: (a) a memory for storing at least one instruction (lines 22-23, Col. 3). The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3)]. Therefore, Claim 62 is rejected for the same rationale as of Claim 1.

ii. Referring to Claims 4, 53, and 58:

As per Claim 4, Fink et al. and Makinson et al. disclose the apparatus of claim 1 comprising:

wherein the classifying comprises determining that data packets of the first type contain real time data [(lines line 12, Col. 3 and lines 18-24, Col. 6 from Makinson et al.)].

As per Claim 53, the rejection of claim 50 is incorporated. In addition, Claim 53 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale as of Claim 4.

As per Claim 58, the rejection of claim 49 is incorporated. In addition, Claim 58 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale as of Claim 4.

iii. Referring to Claims 32, 56, and 60:

As per Claim 32, Fink et al. and Makinson et al. disclose the apparatus of claim 1, wherein the firewall is configured to receive from a packet classification database, information defining the first and second types of data packets [(lines 4-7 and lines 38-41, Col. 8 from Fink et al.)].

As per Claim 56, the rejection of claim 50 is incorporated. In addition, Claim 56 encompasses limitations that are similar to

those of Claim 32. Therefore, it is rejected with the same rationale as of Claim 32.

As per Claim 60, the rejection of claim 49 is incorporated. In addition, Claim 60 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale as of Claim 32.

iv. Referring to Claim 33:

As per Claim 33, Fink et al. and Makinson et al. disclose the apparatus of claim 32, further comprising:

a virus scanning engine configured to receive from a virus detection database, programming information controlling the testing of the data packets of the second type by the virus scanning engine [(line 67, Col. 5 and lines 1-9, Col. 6 from Makinson et al.)].

v. Referring to Claim 34:

As per Claim 34, Fink et al. and Makinson et al. disclose the apparatus of claim 1, further comprising:

a virus scanning engine configured to receive from a virus detection database, programming information controlling the testing of the data packets of the second type by the virus scanning engine [(line 67, Col. 5 and lines 1-9, Col. 6 from Makinson et al.)].

vi. Referring to Claim 40:

As per Claim 40, Fink et al. and Makinson et al. disclose the apparatus of claim 1, further comprising configured to alert the destination upon detection of a virus in the data packets [(lines 30-32, Col. 5 from Makinson et al.)].

vii. Referring to Claim 41:

As per Claim 41, Fink et al. and Makinson et al. disclose the apparatus of claim 1 wherein the destination is a local area network [protected network 12 (Fig. 1 from Fink et al.)].

viii. Referring to Claim 42:

As per Claim 42, Fink et al. and Makinson et al. disclose the apparatus of claim 1 wherein the destination is a personal computer [client computer (Fig. 5 from Makinson et al.)].

ix. Referring to Claim 43:

As per Claim 43, Fink et al. and Makinson et al. disclose the apparatus of claim 1, wherein the destination is a second network [protected network 12 (Fig. 1 from Fink et al.)].

x. Referring to Claim 44:

As per Claim 44, Fink et al. and Makinson et al. disclose the apparatus of claim 1, wherein the first network is a wide area network [external network 14 (Fig 1 from Fink et al.)].

xi. Referring to Claim 45:

As per Claim 45, Fink et al. and Makinson et al. disclose the apparatus of claim 44, wherein the wide area network is the Internet [**External network 14 could optionally be the Internet, for example (lines 28-29, Col. 5 from Fink et al.)**].

xii. Referring to Claim 46:

As per Claim 46, Fink et al. and Makinson et al. disclose the apparatus of claim 1, wherein the destination comprises an Internet service provider configured to connect coupled to a gateway,  
a modem configured to connect to the Internet service provider, and one of a local area or personal computer configured to connect to the modem [**(Fig. 8 from Makinson et al.)**].

xiii. Referring to Claim 47:

As per Claim 47, Fink et al. and Makinson et al. disclose the apparatus of claim 1, further comprising a virus scanning engine configured to decode the data packets during the testing of the data packets [**(lines 4-9, Col. 5 from Makinson et al.) and (lines 4-11, Col. 7 from Fink et al.)**].

xiv. Referring to Claim 48:

As per Claim 48, Fink et al. and Makinson et al. disclose the apparatus of claim 47, wherein the virus scanning engine is configured to function functions as a proxy for a destination processor configured to receive which receives the data packets

**[(lines 25-36, Col. 5 and lines 18-30, Col. 6 from Makinson et al.)].**

xv. Referring to Claim 61:

As per Claim 61, Fink et al. and Makinson et al. disclose the method of claim 49, wherein the classifying is performed by a firewall **[(lines 6-8, Col. 5; lines 65-67, Col. 6; lines 4-7, Col. 8 from Fink et al.)].**

5. Claims 5, 57, 59, and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Makinson et al. (U.S. Patent 7,023,861) and further in view of Lee (U.S. Patent 7,047,561).

i. Referring to Claims 5, 57, 59, and 63:

As per Claim 5, Fink et al. and Makinson et al. disclose the apparatus of claim 4. Fink et al. and Makinson et al. further disclose wherein the classifying comprises determining that data packets of the first type as in Claim 1. Fink et al. and Makinson et al. do not expressly disclose the packets are part of an audio or video data stream. However, Lee discloses the packets are of video or audio content **[(lines 58-62, Col. 1 and lines 36-39, Col. 5 from Lee)].** Fink et al., Makinson et al., and Lee are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been

obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Makinson et al. with Lee et al. to have the video or audio data in the packet(s) communicating in the network environment since one would be motivated to have a firewall for use in association with real-time Internet application (lines 7-8, Col. 1 in Franczek et al.). Therefore, it would have been obvious to modify Fink et al. and Makinson et al. with Lee to obtain the invention as specified in claim 5.

As per Claim 57, the rejection of claim 53 is incorporated. In addition, Claim 57 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

As per Claim 59, the rejection of claim 58 is incorporated. In addition, Claim 59 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

As per Claim 63, the rejection of claim 62 is incorporated. In addition, Claim 63 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

6. Claims 6 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Makinson et al. (U.S. Patent 7,023,861) and further in view of Lyle (U.S. Patent 6,886,012).

i. Referring to Claims 6 and 54:

As per Claim 6, Fink et al. and Makinson et al. disclose the apparatus of claim 1. Fink et al. and Makinson et al. disclose the firewall as in Claim 1. Fink et al. and Makinson et al. do not expressly disclose the remaining limitations of the claim. However, Lyle discloses stop reception of a data stream containing the data packets in response to an alert from the virus scanning engine [(lines 28-34, Col. 14 from Lyle)].

Fink et al., Makinson et al., and Lyle are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Makinson et al. with Lyle to have the various components in the gateway communicating with an alert message if the malicious code is detected, and to stop the data flow into the protected network in such a scenario since one would be motivated to have a way to share information about an attack, dynamically and without human intervention (lines 20-22,

Col. 2 from Lyle). Therefore, it would have been obvious to modify Fink et al. and Makinson et al. with Lyle to obtain the invention as specified in claim 6.

As per Claim 54, the rejection of claim 50 is incorporated. In addition, Claim 54 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale as of Claim 6.

7. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Makinson et al. (U.S. Patent 7,023,861) and further in view of Franczek et al. (U.S. Patent 6,397,335).

i. Referring to Claim 11:

As per Claim 11, Fink et al. and Makinson et al. disclose the apparatus of claim 1. Fink et al. and Makinson et al. do not expressly disclose the remaining limitations of the claim. However, Franczek et al. disclose a buffer [i.e., a **Preferably, each virus-screening processor has an associated memory device to store at least two packets (lines 13-14, Col. 5 from Franczek et al.)**] which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus [(**lines 64-67, Col. 11 from Franczek et al.**)]. Fink et al., Makinson et al., and Franczek

et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Makinson et al. with Franczek et al. to have the stream data in the packet(s) communicating in the network environment since one would be motivated to perform virus screening separately on each of a plurality of virtual channels included in an interactive session (lines 17-19, Col. 12 in Franczek et al.). Therefore, it would have been obvious to modify Fink et al. and Makinson et al. with Franczek et al. to obtain the invention as specified in claim 11.

## Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
  - i. Sonnenberg (U.S. Patent 7,076,650) discloses a method and apparatus are provided for cooperatively and dynamically sharing a proxy's burden of scanning communications for target content. A network of computer nodes is connected to a firewall through which pass communications with entities external to the network. The firewall includes one or more proxies to facilitate network users' connections with the external entities. The firewall and one or more

of the nodes include software modules for scanning one or more types (e.g., FTP, HTTP, SMTP) of communications for particular information or types of data (e.g., computer viruses, ActiveX components, pornography, text). A node having a software module for scanning a communication identifies its scanning capabilities to the firewall. The node may also suggest a class or set of communications that it may scan, which class or set may be defined by its operating parameters or attributes of communications received at the firewall for the node. The firewall negotiates with the node then specifies rules or criteria for determining which communications and under which circumstances the node may scan a communication instead of the firewall. When a communication is received at the firewall and is passed to the proxy, the proxy applies the specified rules to determine which of the proxy and the node should scan the communication. In this manner a substantial amount of communication scanning may be offloaded to individual computer nodes, thereby enhancing or avoiding degradation of the firewall's performance. The division of responsibility between the proxy and any node may be dynamically modified or re-negotiated at virtually any time according to any desired criteria or operating parameters.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone

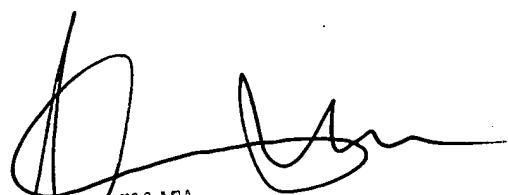
number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Y.C. Shaw

Feb. 01, 2008



KIM VU  
PATENT EXAMINER  
ELECTRONIC BUSINESS CENTER 2135